StreamBIM
By Rendra AS
JDM Technology Group

On Data Security and Digital Construction

A collection of four articles made in connection with Rendra AS attaining ISO 27001 certification and the commercial debut of our on-prem security solutions.
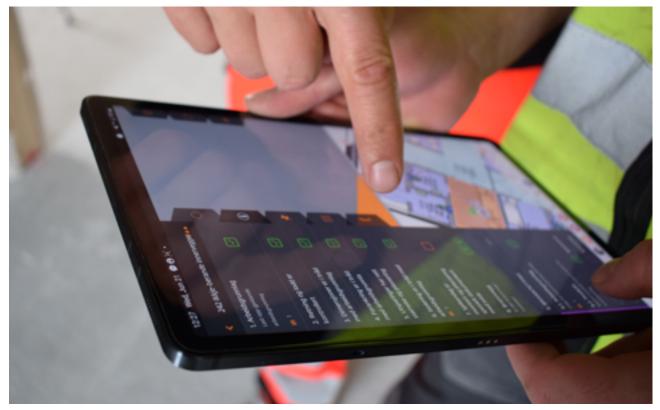
StreamBIM handles large quantities of our customers' sensitive data.

Article 1

Rendra AS is ISO/IEC 27001 certified
- We work systematically with data security.

In a world increasingly exposed to physical and cyber threats, construction industry stakeholders are becoming more aware of the need to protect their data. Given that the physical assets we design, construct and operate will last for many years, and that the data describing these assets is more mobile and consumable than ever before in the digital formats of today, safeguarding our physical assets requires more diligence than ever before.

One of the tenets of BIM is that sharing data with project participants and democratising project data is advantageous for the design and production processes. We want people to read from the same page and have the same understanding of the intended result. On the other hand, uncritical sharing of data

can lead to breaches. Projects must be aware that their data needs to be protected in the same way as they would secure their building sites. Access should only be granted to the people who have a job to do inside the perimeter fence. a more robust training system and better documentation.

We are proud to have achieved ISO/IEC 27001 certification for our ongoing work on securing our systems and data against all threats. Our customers and partners can rely on us at Rendra to continue doing our utmost to protect their data in StreamBIM.

As a result of all the charting, formalisation and documentation work leading up to the certification Rendra and our subsidiaries have gained a stronger and more systematic ISMS, which instils more trust in us by our customers and users, and in turn their end-clients and partners.

Customers looking for data management solutions that protect their data need confidence that the systems entrusted with their data are secure and managed appropriately. An Information Security Management System (ISMS) is a good response to these requirements. ISO 27001 formalises the structure of an ISMS. Certifying according to the standard demonstrates to customers and users alike that an organisation takes information security seriously and continually works to maintain and improve routines.

Why we spent so much time and resources on certification

The certification strengthens our obligation to provide first-rate BIM solutions in StreamBIM that not only are innovative and user friendly, but also secure and reliable.

We have maintained a high focus on data security since our founding in 2012, but in a digital world that is becoming ever more precarious, it is important to document that we make every effort to protect our systems against unfriendly actors who might want to exploit any security gap for whatever nefarious reason.

'We in Rendra have always had a focus on data security and worked continuously on protecting our customers' data. We are proud that we now have formalised our ongoing work with the ISO/IEC 27001 certification, says Ole Kristian Kvarsvik, Managing Director of Rendra AS. We will redouble our efforts on data security and maintain the quality our customers' expect, so StreamBIM will continue to be the best - and most secure - collaboration platform on the market.'

Ole Kristian Kvarsvik, Managing Director Rendra AS

Some of our customers are required to document that their systems are secure against data breaches, either in general or for certain projects, and are in practice forced to choose systems that are ISO/IEC 27001 certified. For us at Rendra, this has been a good opportunity to better chart the risks we face and formalise and shore up our routines and have them scrutinised by a third-party audit.

What we have done

During the certification process we have taken all our preexisting routines and processes and formalised and documented them, in addition to enforcing a more stringent control system. This gives us more robust and verifiable routines to handle current and future data security threats.

Included in this are strict guidelines for access control, data encryption, regular revisions and systems maintenance, as well as a more systematic training programme for Rendra staff to increase their focus on data security.

What we have learned

Data security has always been part of Rendra's DNA. The streaming of building data from data centres to PCs and handheld devices has forced us to think about data security from the very beginning. Through access controls, we can ensure that only the relevant project data is being made available to only those who need to access it, and no one outside the project. We can further secure the data by disabling file downloads from projects.

'For us at Rendra, the process of certifying to ISO 27001 has been fun! As I joined the organisation in 2021 and started the certification process in 2023, it has been very encouraging to see that solid foundations for an ISMS were already laid. Essentially, the task now was to demonstrate compliance with ISO 27001 by documenting the existing technical measures and describing organisational procedures.'

Rupert Hanna, Chief Implementation Officer at Rendra

During the certification process you learn that certification itself is not the end goal. Once an organisation is certified, the journey begins. Certification requires an organisation to continuously improve its procedures and systems, assess new and existing risks and follow its own procedures. Often, the weakest link in information security is the people who handle the data. Proper training of the entire organisation is key to ensuring the principles of information security and how to apply them in the context of operations.

It's not the system that is certified, it's the organisation.

StreamBIM offline On-Prem lets you enjoy the benefits of digital construction on-site with maximum data security.

Article 2

StreamBIM On-Prem (offline)

As contractors and building owners the world over are rapidly adopting digital construction methods and not turning back, data security for the cloud-based digital tools they use is becoming ever more important. We at Rendra focus on maintaining a high level of data security in every project being run in 'regular' StreamBIM, but we do recognize that some projects need higher levels of security than others, either by customer preference or statutory requirement.

We have found that there is a substantial market demand for digital solutions that can be used even under the strictest of security conditions, and our response is the offline StreamBIM On-Prem configuration. Developed in close cooperation with our customers and tailored to the real needs of their highly confidential projects, our unique solution is certainly piquing a lot of interest and turning out to be a strategically important product range for Rendra and our subsidiaries.

Tailoring a solution for your project's needs

StreamBIM has several features that facilitate an increasing level of security, and which lets us tailor a solution to fit the needs of any project. Going for the high end offline on-prem is a significant strategic choice for a project, so the customers that use the solution are typically the building owners themselves or the main contractor.

The configuration is normally reserved for sensitive projects of national importance or critical business value. Examples are; central government buildings, military in-stallations, critical power infrastructure, high-end manufacturing facilities and data centres.

StreamBIM On-Prem was originally developed in cooperation with one of our central customers with a specific project in mind; a project where running software on a completely fenced-off confidential network was mandated by law.

We now see a great deal of demand for this solution in several markets, and having already done all the hard work, we can now let other customers benefit from it.

Ole Kristian Kvarsvik, Managing Director at Rendra AS

A completely fenced-off, secure environment

In a world where data security is always being tested by unfriendly actors, the only proper guarantee we have against having project data compromised is to have the system completely fenced off from the internet. As a cloud-based platform, this of course presented some challenges for us, but we have created an installation pack-age that can be run on an offline server in a secure (on-site) location on a confidential network - in effect creating a fenced-off mini StreamBIM that can only be accessed from within the confidential network it is installed in.
Typically, access is limited to the customer's in-house project team only, which lets the projects benefit from StreamBIM functionality while still enjoying maximum secu-rity and giving project management some peace of mind.

In the most secure configurations, workers on-site will work with StreamBIM on of-fline tablets that are docked and synced overnight. The information stored locally is secondary and compartmentalised, so each worker will only have access to the information that is relevant for their current daily work routine.

Standard StreamBIM

Data is processed in the cloud, on a national or regional server, then encrypted and streamed to all devices via mobile networks or WiFi

StreamBIM Offline On-prem

Data is processed on an on-site server, then encrypted and transmitted to devices on a cabled, confidential network. Tablets are docked and synced at set intervals.

On-site workers only access and handle relevant data

Benefits and challenges of offline on-prem

Going offline on-prem will secure your data at the same time as your project benefits from the increases in efficiency and control that digital construction offers, but there are some challenges that must be considered before deciding on a configuration. Running a single-project or single-customer installation on a separate server will of course mean increased costs compared with using StreamBIM 'out of the box' on our standard servers, but for the types of projects with very strict security requirements it is usually considered from the very beginning.

There can be operational challenges if Rendra staff do not have access to the server environment or data. Troubleshooting problems, such as issues with IFC files, must be done by the customer's in-house project team themselves, which may require specific expertise. Even with cooperation from our experts, the resolve time is usually increased. StreamBIM is a complex system, and operating and monitoring the system requires competence from the customer's IT department or other with physical presence/access to the on-prem environment.

Usually, only projects that are confidential by law will require this level of physical security on all levels, so for sensitive projects not quite on the level of offline on-prem, please check out our various versions of the (slightly) more forgiving **StreamBIM On-prem (online)** solution which enables us at Rendra to remotely run, monitor and bugfix.

To sum up; StreamBIM offline On-Prem is a market-leading solution for digital construction that can accommodate even the most stringent of security requirements. Combining the best of the digital age and the oldest security measures in the book, offline On-Prem lets a confidential project benefit from intuitive site tools, increased efficiency, improved oversight and fewer mistakes - like in all StreamBIM projects - at the same time as data security is maintained in a physically fenced-off environment. There are few alternatives to StreamBIM if you want to do digital construction in a secure environment.

StreamBIM online On-Prem lets you enjoy the benefits of working in a cloud-based solution while minimising data exposure to the wider world of third-party networks.

Article 3

StreamBIM On-Prem (online)

The construction industry is rapidly moving towards digital construction, making data security for the digital tools that are being used ever more important. We at Rendra focus on maintaining a high level of data security in every project being run in 'regular' StreamBIM, but we do recognize that some projects need higher levels of security. Unfriendly actors are always testing defences, so there is an ever-increasing market demand for digital solutions that can be used for highly confidential construction projects.

Balancing connectivity and security with a private cloud

As a cloud-based platform this of course presented some challenges for StreamBIM, but our response was to develop offline StreamBIM On-Prem configuration in cooperation with some of our customers. Not all projects have the statutory requirements that often necessitates running the completely fenced-off offline solution, but project owners may still want the increased security that comes from run-

ning an isolated system. This is why we also have a hybrid version that maintains the best of both worlds. The main difference between the two solutions is that the online version lets Rendra staff install and maintain the system via a secure link to your server, removing the need for costly in-person appearances on-site.

Tailoring a solution for your project's needs

Having somewhat fewer constraints than a completely offline solution allows the project owner more freedom to combine various security features into a configuration that is adapted to preference and budget. StreamBIM has several configurations and optional features that facilitate an increasing level of security.

The online on-prem solution, in its many variants, is relevant for customers that have sensitive projects of national importance or critical business value. Examples are; government buildings, military installations, civil and power infrastructure, research or industrial facilities, data centres, museums, prisons and banking facilities.

"The various configurations available for StreamBIM online On-Prem makes this a much more flexible solution compared with the completely fenced-off offline version, while still maintaining superior data security. The key here is reducing outside data traffic as much as possible while introducing additional security measures when external traffic is unavoidable.
This flexibility makes it easier to adapt to our customers' needs and budgets by tailoring a setup to the specific StreamBIM project."

Ole Kristian Kvarsvik, Managing Director at Rendra AS

A secure work environment in a private cloud.

The most common StreamBIM online On-Prem configuration is to use a local Wi-Fi network with good security measures and typically inside customer firewalls. While not as secure as a completely fenced-off and offline system, it allows outside and off-site stakeholders to connect via secure links while minimising data traffic outside of the controlled environment. The great advantage of the online On-prem installation vs. the offline one, is that our development team can access the server and operate it remotely.

Combined with other security measures this will satisfy the requirements for most confidential projects, letting projects benefit from all parties using digital tools on-site at the same time as project management can maintain their beauty sleep.

Standard StreamBIM

Data is processed in the cloud, on a national or regional server, then encrypted and streamed to all devices via mobile networks or WiFi

StreamBIM Online On-prem

Data is processed on an on-site server, then encrypted and transmitted to devices via secure WiFi only. Outside access by secure link may be available, depending on the chosen setup.
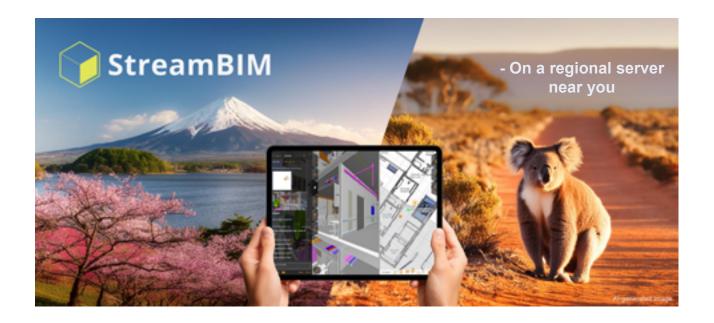
Benefits and challenges of online on-prem

Running a single-project or single-customer installation on a separate server will of course entail an increased cost compared with using StreamBIM 'out of the box' on our standard servers, but the online on-prem solution is a good compromise that minimises the extra cost while still maintaining a very high level of security.

The flexibility inherent in this set-up lets our customers configure a package that fits their security requirements while keeping an eye on the budget. Some very high security projects also require physical security on all levels, so for more information on these, please check out our StreamBIM On-prem (offline) solution.

To sum up; StreamBIM online On-Prem is a market-leading solution for digital construction that can accommodate strict security requirements. By running in a private cloud, we are minimising unnecessary access to the system from the outside, providing fewer angles of attack for malevolent actors. Confidential projects can still benefit from intuitive site tools, increased efficiency, improved oversight and fewer mistakes - like in any other StreamBIM project – all the while making data security a priority.

Article 4

National and regional StreamBIM servers; from a data security perspective

A good cloud-based service must always balance between making the service as easy and convenient as possible for the customer, while maintaining strict standards for data security. As the construction industry is rapidly moving towards digital construction, building trust in the digital tools that are being used - and securing the underlying data - is paramount, even if the end-users may grumble a bit at some of the measures being an inconvenience in their daily use.

These security features are not the end-all of data security, though. We at Rendra put great weight on maintaining a high level of data security in every project being run in StreamBIM, and part of this is also having a focus on the wider context we operate in.

StreamBIMs regional servers

The primary reason for setting up regional servers is functional; to reduce latency, i.e. to improve performance, for our users and to comply with data-residency requirements. While the basic downloading of data depends more on your internet

connection than distance, operations that entail data traffic going back and forth to the database, like advanced queries, will experience a performance hit when using a distant server.

This is main reason for why we set up our Japan server as well as the newly established Australian server, which are now the primary servers for their respective national and regional areas.

However, closeness to a given market cannot be the only variable we consider when choosing new server locations. When securing our customers' data, the framework surrounding the data storage is equally important.

The choice of the server provider

All the time we at Rendra don't run our own server parks, we cooperate with trustworthy, well established third-party providers that we can rely on, as they will be the final, physical line of security for our customers' data. This mostly means using servers run by well-known international providers, using first-rate data centres. One of the advantages of using this type of provider it that they have experience in providing a stable service, established security routines and they usually build and manage their own server parks. Choosing a provider with many international locations is also a convenience for our technical staff, as having coherent systems across our server locations makes our software and database maintenance easier and more predictable.

Data residency

A topic that is becoming more and more important for both our customers and their end-clients is data residency. Storing data in an unspecified offshore location may allow too many vectors of attack for unfriendly actors, especially during data transmission across continents. For sensitive projects of a national importance such as government and security installations, critical infrastructure, or projects of a central business importance like data centres and industrial facilities, having the possibility to keep one's data close at hand is a consideration for end-clients when choosing a SaaS solution.

For StreamBIM, requirement for domestic data residency may mean having to set up a 'private cloud' on-prem server for a specific customer, or if we have several

customers with these requirements, establish national servers for countries that are already served by a regional server.

An example in point would be the new Swedish StreamBIM server. Most Swedish projects still run on the main EU server and are well served there, but market requirements made having a domestic alternative a necessity, as many sensitive projects in Sweden require domestic data storage. Often, this server is also required to be domestically owned, even precluding the usually go-to international providers.

'Here in Japan, we find that many of our customers' end-clients - especially the large corporations - have very strict data security requirements. For us this means a steady flow of vetting procedures to allow the use of StreamBIM in certain projects, and data residency is one of the questions that crops up again and again. If we didn't have a Japanese server, it could be rather difficult for our customers to gain the trust of many of their clients in a SaaS solution such as ours.'

Jostein Edvardsen, Country Manager, StreamBIM Japan

The importance of storing data in a politically stable location

Last, but not least, we always store our customers' data in countries that have a stable political system and a well-established rule of law. Especially when serving several different markets on a regional server, we must store the data in a jurisdiction where our customers will have good legal rights, where there are clear cut rules on both data- and individual privacy, which again will be enforced by an independent judicial system. We are acutely aware that storing data in a place where the local government or other actors could extra-judicially access customer data would be ruinous for the trust that a cloud computing solution like StreamBIM requires.

To sum up; we at Rendra work tirelessly to continuously improve StreamBIM and provide our customers with the data security they need. This work does not just focus on the software itself, but also on company-internal factors, like our attaining ISO 27001 certification. External factors, such as the location of our servers and the providers we choose to work with, is becoming ever more important for our customers and their end-clients, so StreamBIM in turn must always adapt to anticipate and meet their data security needs.

StreamBIM Japan Co., Ltd.

Get in touch

If you have any questions about our services or StreamBIM in particular, or Scandinavian digital construction in general, please get in touch!

Email: japan@streambim.com

**Make a free trial on our Japan server
by following the link below.**

https://streambim.com/html/jp/free-trial.html

If you have any questions, or would like to test additional features, please contact our support team using the in-app support chat, or email us at japan@streambim.com

[Google play] [App Store]

Rendra AS

Head office: Østre Aker vei 17
              0581 Oslo, Norway
Mail to: Po.Box 688 Løren
              0507 Oslo, Norway

StreamBIM Japan Co., Ltd.

Kamiyacho Trust Tower (23F WWJ)
4-1-1 Toranomon, Minato-ku
Tokyo 105-6923, Japan

www.streambim.com